Smernice



Smernice št. 04/2020 o uporabi lokacijskih podatkov in orodij za sledenje stikom v okviru izbruha COVID-19

Sprejete 21. aprila 2020

sprejeto

Zgodovina različic

Različica 1.1	5. maj 2020	Manjši popravki
Različica 1.0	21. april 2020	Sprejetje smernic

Kazalo

Evropski odbor za varstvo podatkov je –

ob upoštevanju člena 70(1)(e) Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljevanju: Splošna uredba o varstvu podatkov),

ob upoštevanju Sporazuma EGP ter zlasti Priloge XI in Protokola 37 k Sporazumu EGP, kakor sta bila spremenjena s Sklepom Skupnega odbora EGP št. 154/2018 z dne 6. julija 2018[1],

ob upoštevanju členov 12 in 22 svojega poslovnika –

SPREJEL NASLEDNJE SMERNICE:

1 UVOD IN OZADJE

1 Vlade in zasebni akterji se pri odzivu na pandemijo COVID-19 usmerjajo k uporabi rešitev, utemeljenih na podatkih, kar vzbuja številne pomisleke glede zasebnosti.

2 Evropski odbor za varstvo podatkov poudarja, da je bil pravni okvir za varstvo podatkov zasnovan tako, da je prožen, in zato lahko omogoča učinkovit odziv pri omejevanju pandemije ter varstvo temeljnih človekovih pravic in svoboščin.

3 Evropski odbor za varstvo podatkov je trdno prepričan, da je pri obdelavi osebnih podatkov, ki je potrebna za obvladovanje pandemije COVID-19, varstvo podatkov nujno za vzpostavitev zaupanja, ustvarjanje pogojev za družbeno sprejemljivost katere koli rešitve in s tem tudi zagotovitev učinkovitosti takšnih ukrepov. Virus ne pozna meja, zato se zdi primerneje, da se na sedanjo krizo odzovemo z razvojem skupnega evropskega pristopa ali vsaj vzpostavitvijo interoperabilnega okvira.

4 Evropski odbor za varstvo podatkov na splošno meni, da bi bilo treba podatke in tehnologijo v boju proti COVID-19 uporabiti za krepitev vloge posameznikov in ne za njihovo nadziranje, stigmatiziranje ali omejevanje. Podatki in tehnologija so sicer lahko pomembna orodja, vendar imajo svoje omejitve in lahko zgolj povečajo učinkovitost drugih javnozdravstvenih ukrepov. Vsi ukrepi, ki jih sprejmejo države članice ali institucije EU in ki vključujejo obdelavo osebnih podatkov za boj proti COVID-19, morajo biti utemeljeni na splošnih načelih učinkovitosti, nujnosti in sorazmernosti.

5 Te smernice pojasnjujejo pogoje in načela za sorazmerno uporabo lokacijskih podatkov in orodij za sledenje stikom za dva posebna namena:

- uporaba lokacijskih podatkov v podporo odzivu na pandemijo z modeliranjem širjenja virusa, da se oceni splošna učinkovitost ukrepov za osamitev;
- sledenje stikom, katerega namen je obveščanje posameznikov o dejstvu, da so bili v neposredni bližini osebe, za katero se potrdi, da je nosilec virusa, in sicer s ciljem, da se čim prej prekinejo verige okužb.

6 Učinkovitost prispevka aplikacij za sledenje stikom k obvladovanju pandemije je odvisna od več dejavnikov (npr. odstotka oseb, ki bi morale aplikacije namestiti na svoje naprave, opredelitve pojma „stik“ v smislu razdalje in trajanja). Poleg tega morajo biti take aplikacije del celovite strategije javnega zdravja za boj proti pandemiji, ki med drugim vključuje testiranje in naknadno ročno sledenje stikom z namenom odprave dvoma. Njihovo uvajanje bi morali

[1] Sklicevanja na „države članice“ v tem dokumentu so mišljena kot sklicevanja na „države članice EGP“.

spremljati podporni ukrepi za zagotovitev, da se uporabnikom zagotovijo kontekstualizirane informacije in da opozorila lahko koristijo sistemu javnega zdravja. V nasprotnem primeru te aplikacije morda ne bodo tako učinkovite, kot bi lahko bile.

7 Evropski odbor za varstvo podatkov poudarja, da tako Splošna uredba o varstvu podatkov kot tudi Direktiva 2002/58/ES (v nadaljevanju: Direktiva) vsebujeta posebna pravila, ki omogočajo uporabo anonimnih ali osebnih podatkov, da se podprejo javni organi in drugi akterji na nacionalni ravni in ravni EU pri spremljanju in omejevanju širjenja virusa SARS-CoV-2[2].

8 V zvezi s tem je Evropski odbor za varstvo podatkov že sprejel stališče, da bi morala biti uporaba aplikacij za sledenje stikom prostovoljna in se ne bi smela opirati na spremljanje gibanja posameznikov, temveč na informacije o medsebojni bližini uporabnikov[3].

[2] Glej predhodno izjavo Evropskega odbora za varstvo podatkov o izbruhu COVID-19.
[3] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf.

2 UPORABA LOKACIJSKIHPODATKOV

2.1 Viri lokacijskih podatkov

9 Za modeliranje širjenja virusa in splošno učinkovitost ukrepov za osamitev sta na voljo dva glavna vira lokacijskih podatkov:

- lokacijski podatki, ki jih pri nudenju svojih storitev zbirajo ponudniki elektronskih komunikacijskih storitev (kot so operaterji mobilnih telekomunikacij), in
- lokacijski podatki, ki jih zbirajo aplikacije ponudnikov storitev informacijske družbe, ki za svoje delovanje potrebujejo uporabo takih podatkov (npr. navigacija, prevozne storitve itd.).

10 Evropski odbor za varstvo podatkov opozarja, da se lokacijski podatki[4], ki se zberejo od ponudnikov elektronskih komunikacijskih storitev, lahko obdelujejo samo v skladu s členoma 6 in 9 Direktive. To pomeni, da se lahko ti podatki posredujejo organom ali drugim tretjim osebam le, če jih je ponudnik anonimiziral ali, v primeru podatkov, ki razkrivajo zemljepisni položaj terminalske opreme uporabnika in niso podatki o prometu, če je uporabnik predhodno v to privolil[5].

11 Za informacije, ki se zbirajo neposredno s terminalske opreme, vključno z lokacijskimi podatki, se uporablja člen 5(3) Direktive. Shranjevanje informacij na napravi uporabnika ali dostopanje do že shranjenih informacij je zato dovoljeno le, če (i) je uporabnik v to privolil[6] ali (ii) sta shranjevanje in/ali dostop nujno potrebna za storitev informacijske družbe, ki jo je uporabnik izrecno zahteval.

12 Odstopanja od pravic in obveznosti, določenih v Direktivi, pa so mogoča v skladu s členom 15, kadar pomenijo potreben, primeren in sorazmeren ukrep znotraj demokratične družbe za določene cilje[7].

13 Za vnovično uporabo lokacijskih podatkov, ki jih zbira ponudnik storitev informacijske družbe za namene modeliranja (npr. prek operacijskega sistema ali neke predhodno nameščene aplikacije), morajo biti izpolnjeni dodatni pogoji. Kadar se podatki zbirajo v skladu s členom 5(3) Direktive, se lahko nadalje obdelajo le z dodatno privolitvijo posameznika, na katerega se nanašajo osebni podatki, ali na podlagi prava Unije ali prava države članice, ki pomeni potreben in sorazmeren ukrep v demokratični družbi za zaščito ciljev iz člena 23(1) SUVP[8].

2.2 Poudarek na uporabi anonimiziranih podatkov o lokaciji

14 Evropski odbor za varstvo podatkov poudarja, da bi bilo treba pri uporabi lokacijskih podatkov vedno dati prednost obdelavi anonimiziranih podatkov in ne obdelavi osebnih podatkov.

15 Anonimizacija se nanaša na uporabo množice tehnik, s katerimi se onemogoči, da se podatki z „razumnim" naporom povežejo z določenim ali določljivim posameznikom. Pri tem preizkusu „razumnosti" je treba upoštevati tako objektivne vidike (čas, tehnična sredstva) kot tudi kontekstualne elemente, ki so lahko različni glede na posamičen primer (redkost pojava, ki upošteva npr. gostoto prebivalstva, naravo in količino podatkov). Če podatki tega preizkusa ne prestanejo, niso bili anonimizirani in zato ostanejo vključeni v področje uporabe Splošne uredbe o varstvu podatkov.

16 Ocenjevanje zanesljivosti anonimizacije temelji na treh merilih: (i) izločitev (osamitev posameznika znotraj večje skupine na podlagi podatkov); (ii) povezljivost (povezovanje dveh

---

[4] Glej člen 2(c) Direktive.
[5] Glej člena 6 in 9 Direktive.
[6] Pojem privolitve v Direktivi ostaja isti kot pojem privolitve v Splošni uredbi o varstvu podatkov in mora izpolnjevati vse zahteve za privolitev iz členov 4(11) in 7 Splošne uredbe o varstvu podatkov.
[7] Za razlago člena 15 Direktive glej tudi sodbo Sodišča Evropske unije z dne 29. januarja 2008 v zadevi C-275/06, *Productores de Música de España (Promusicae) proti Telefónica de España SAU.*
[8] Glej razdelek 1.5.3 Smernic št. 1/2020 o obdelavi osebnih podatkov v zvezi s povezanimi vozili.

zapisov, ki se nanašata na istega posameznika) in (iii) sklepanje (deduciranje, z znatno verjetnostjo, neznanih informacij o posamezniku).

17 Pojem anonimizacije se pogosto napačno razume in zamenjuje s psevdonimizacijo. Anonimizacija omogoča uporabo podatkov brez kakršnih koli omejitev, psevdonimizirani podatki pa ostajajo vključeni v področje uporabe Splošne uredbe o varstvu podatkov.

18 Obstaja več možnosti za učinkovito anonimizacijo[9], vendar s pridržkom. Podatkov ni mogoče anonimizirati posamično, kar pomeni, da je mogoče anonimizirati samo celotne sklope podatkov. V tem smislu se vsak poseg na posamičnem vzorcu podatkov (s šifriranjem ali katero koli drugo matematično pretvorbo) lahko v najboljšem primeru šteje za psevdonimizacijo.

19 Postopki anonimizacije in napadi s ciljem vnovične identifikacije so aktivna raziskovalna področja. Ključno je, da vsak upravljavec, ki izvaja rešitve za anonimizacijo, spremlja najnovejša spoznanja na tem področju, zlasti v zvezi z lokacijskimi podatki (ki izvirajo iz telekomunikacijskih operaterjev in/ali storitev informacijske družbe), za katere je znano, da jih je zelo težko anonimizirati.

20 Dejansko je veliko raziskav pokazalo[10], da *lokacijski podatki, za katere se domneva, da so anonimizirani*, to morda sploh niso. Sledi mobilnosti posameznikov so med seboj tesno povezane in edinstvene. Zato so lahko v nekaterih okoliščinah dovzetne za poskuse vnovične identifikacije.

21 Posamičnega vzorca podatkov o sledenju lokaciji posameznika v daljšem času ni mogoče popolnoma anonimizirati. Ta ocena lahko še vedno velja, če se natančnost zabeleženih zemljepisnih koordinat ne zmanjša dovolj ali če se podatki o sledeh odstranijo in tudi če se hranijo samo podatki o lokacijah, na katerih se posameznik, na katerega se nanašajo osebni podatki, zadržuje dlje časa. To velja tudi za slabo agregirane lokacijske podatke.

22 Da bi dosegli anonimizacijo, je treba lokacijske podatke skrbno obdelati, da prestanejo preizkus razumnosti. V tem smislu taka obdelava vključuje upoštevanje sklopov lokacijskih podatkov kot celote in obdelavo podatkov iz razumno velikega sklopa posameznikov z uporabo razpoložljivih zanesljivih tehnik anonimizacije, pod pogojem, da se ustrezno in učinkovito izvajajo.

23 Zaradi zapletenosti postopkov anonimizacije se zelo spodbuja preglednost v zvezi z metodologijo anonimizacije.

---

[9] De Montjoye et al., 2018, „On the privacy-conscientious use of mobile phone data“.
[10] De Montjoye et al., 2013, „Unique in the Crowd: The privacy bounds of human mobility“ in Pyrgelis et al., 2017, „Knock Knock, Who’s There? Membership Inference on Aggregate Location Data“.

3 APLIKACIJE ZA SLEDENJE STIKOM

3.1 Splošna pravna analiza

24 Sistematično in obsežno spremljanje lokacije in/ali stikov posameznikov močno posega v njihovo zasebnost. Upraviči se lahko le z opiranjem na to, da ga uporabniki prostovoljno sprejmejo za vsak posamezen namen. To bi pomenilo zlasti, da posamezniki, ki se odločijo, da takih aplikacij ne bodo uporabljali, ali ki jih ne morejo uporabljati, ne bi smeli imeti negativnih posledic.

25 Za zagotovitev odgovornost bi bilo treba za vsako aplikacijo za sledenje stikom jasno opredeliti upravljavca. Evropski odbor za varstvo podatkov meni, da bi upravljavci[11] za tako aplikacijo lahko bili nacionalni zdravstveni organi; predvidijo se lahko tudi drugi upravljavci. V vsakem primeru pa je treba, če uvedba aplikacij za sledenje stikom vključuje različne akterje, od vsega začetka jasno določiti njihove vloge in odgovornosti ter jih pojasniti uporabnikom.

26 Poleg tega, kar zadeva načelo omejitve namena, morajo biti nameni dovolj specifični, da se izključi nadaljnja obdelava za namene, ki niso povezani z obvladovanjem zdravstvene krize COVID-19 (npr. komercialni nameni ali nameni kazenskega pregona). Po jasni opredelitvi cilja bo treba zagotoviti, da je uporaba osebnih podatkov ustrezna, potrebna in sorazmerna.

27 V zvezi z aplikacijo za sledenje stikom bi bilo treba skrbno upoštevati načelo najmanjšega obsega podatkov ter načelo vgrajenega in privzetega varstva podatkov:

- za aplikacije za sledenje stikom ni potrebno sledenje lokaciji posameznih uporabnikov. Namesto tega bi bilo treba uporabiti podatke o bližini;
- ker lahko aplikacije za sledenje stikom delujejo brez neposredne identifikacije posameznikov, bi bilo treba uvesti ustrezne ukrepe za preprečevanje vnovične identifikacije;
- zbrane informacije bi bilo treba shranjevati na terminalski opremi uporabnika, zbirati pa bi bilo treba samo relevantne informacije, kadar je to zares nujno potrebno.

28 Glede zakonitosti obdelave Evropski odbor za varstvo podatkov ugotavlja, da aplikacije za sledenje stikom vključujejo shranjevanje in/ali dostop do informacij, ki so že shranjene na terminalski napravi, za katera velja člen 5(3) Direktive. Če so ta dejanja nujna, da bi ponudnik aplikacije lahko zagotovil storitev, ki jo je uporabnik izrecno zahteval, za obdelavo ne bi bila potrebna privolitev uporabnika. Za dejanja, ki niso nujno potrebna, bi moral ponudnik pridobiti privolitev uporabnika.

29 Poleg tega Evropski odbor za varstvo podatkov ugotavlja, da samo dejstvo, da je uporaba aplikacij za sledenje stikom prostovoljna, ne pomeni, da bo obdelava osebnih podatkov nujno temeljila na privolitvi. Kadar javni organi zagotavljajo storitev na podlagi pooblastila, ki jim je podeljeno in je v skladu z zakonsko določenimi zahtevami, se zdi, da je najbolj ustrezna pravna podlaga za obdelavo ta, da je obdelava potrebna za opravljanje naloge v javnem interesu, tj. člen 6(1)(e) Splošne uredbe o varstvu podatkov.

30 V členu 6(3) Splošne uredbe o varstvu podatkov je pojasnjeno, da se podlaga za obdelavo iz člena 6(1)(e) določi v skladu s pravom Unije ali pravom države članice, ki velja za upravljavca. Namen obdelave se določi v navedeni pravni podlagi ali pa je ta v primeru obdelave iz točke (e) odstavka 1 potrebna za opravljanje naloge, ki se izvaja v javnem interesu, ali pri izvajanju javne oblasti, dodeljene upravljavcu[12].

31 Vendar bi morala pravna podlaga ali zakonodajni ukrep, ki pomeni zakonito podlago za uporabo aplikacij za sledenje stikom, vključevati smiselne zaščitne ukrepe, vključno s sklicem na prostovoljnost uporabe aplikacije. Vključiti bi bilo treba jasno opredelitev namena in

---

[11] Glej tudi dokument Evropske komisije „Usmeritve v zvezi z varstvom podatkov za aplikacije, ki podpirajo boj proti pandemiji COVID-19“, Bruselj, C(2020) 2523 konč. z dne 16. aprila 2020.
[12] Glej uvodno izjavo 41.

izrecne omejitve glede nadaljnje uporabe osebnih podatkov ter jasno opredeliti udeležene upravljavce. Opredeliti bi bilo treba tudi vrste podatkov in subjekte, ki se jim osebni podatki lahko razkrijejo (ter za katere namene). Odvisno od ravni poseganja bi bilo treba vključiti dodatne zaščitne ukrepe, pri čemer je treba upoštevati naravo, obseg in namene obdelave. Evropski odbor za varstvo podatkov prav tako priporoča, da se v najkrajšem možnem času vključijo merila za določitev, kdaj se bo aplikacija ukinila in kateri subjekt bo odgovoren za sprejetje te odločitve.

32 Če pa obdelava podatkov temelji na drugi pravni podlagi, na primer privolitvi (člen 6(1)(a))[13], bo moral upravljavec zagotoviti, da so izpolnjene stroge zahteve za veljavnost te pravne podlage.

33 Poleg tega bi uporaba aplikacije v boju proti pandemiji COVID-19 lahko privedla do zbiranja zdravstvenih podatkov (na primer statusa okužene osebe). Obdelava takih podatkov je dovoljena, kadar je potrebna iz razlogov javnega interesa na področju javnega zdravja, pri čemer morajo biti izpolnjeni pogoji iz člena 9(2)(i) Splošne uredbe o varstvu podatkov[14], ali za namene zdravstvene oskrbe, kot je opisano v členu 9(2)(h) Splošne uredbe o varstvu podatkov[15]. Odvisno od pravne podlage lahko obdelava temelji tudi na izrecni privolitvi (člen 9(2)(a) Splošne uredbe o varstvu podatkov).

34 V skladu s prvotnim namenom člen 9(2)(j) Splošne uredbe o varstvu podatkov omogoča tudi obdelavo zdravstvenih podatkov, kadar je potrebna za znanstvenoraziskovalne ali statistične namene.

35 Sedanje zdravstvene krize ne bi smeli izrabiti kot priložnost za uvajanje nesorazmernih pooblastil za hrambo podatkov. Pri omejitvi hrambe bi bilo treba upoštevati dejanske potrebe in zdravstveno pomembnost (to lahko vključuje epidemiološke vidike, kot je inkubacijska doba), osebne podatke pa bi bilo treba hraniti samo v času trajanja krize COVID-19. Potem bi bilo treba vse osebne podatke praviloma izbrisati ali anonimizirati.

36 Evropski odbor za varstvo podatkov meni, da take aplikacije ne morejo nadomestiti, temveč lahko le podprejo ročno sledenje stikom, ki ga izvaja usposobljeno javnozdravstveno osebje, ki lahko ugotovi, ali je verjetno, da tesni stiki povzročijo prenos virusa, ali ne (npr. interakcija z osebo, ki je zaščitena z ustrezno opremo – blagajniki itd. – ali ki ni zaščitena). Evropski odbor za varstvo podatkov poudarja, da bi morali biti postopki in procesi, vključno z ustreznimi algoritmi v aplikacijah za sledenje stikom, pod strogim nadzorom usposobljenega osebja, da se omeji pojavljanje lažno pozitivnih in lažno negativnih rezultatov. Zlasti naloga zagotavljanja svetovanja o naslednjih korakih ne bi smela temeljiti zgolj na avtomatizirani obdelavi.

37 Za zagotovitev njihove pravičnosti, upravičljivosti in, širše, skladnosti z zakonodajo morajo biti algoritmi preverljivi in bi jih morali redno pregledovati neodvisni strokovnjaki. Izvorna koda aplikacije bi morala biti javno dostopna za najširši možni nadzor.

38 Lažno pozitivni rezultati se bodo v nekem obsegu vedno pojavljali. Ker lahko ugotavljanje tveganja okužbe na posameznike verjetno močno vpliva, na primer, da ostanejo v samoosamitvi, dokler ni rezultat testa negativen, je nujno uvesti možnost popravljanja podatkov in/ali naknadnih rezultatov analize. To bi seveda moralo veljati le za scenarije in izvedbe, v katerih se podatki obdelujejo in/ali shranjujejo na način, ki s tehničnega vidika omogoča tak popravek, in v katerih je verjetno, da bodo nastali zgoraj navedeni negativni učinki.

[13] Upravljavci (zlasti javni organi) morajo posebno pozornost nameniti dejstvu, da se privolitev ne bi smela šteti za prostovoljno, če posameznik nima prave možnosti izbire, da zavrne ali prekliče svojo privolitev, ne da bi mu to povzročilo škodo.

[14] Obdelava mora temeljiti na pravu Unije ali pravu države članice, ki zagotavlja ustrezne in posebne ukrepe za zaščito pravic in svoboščin posameznika, na katerega se nanašajo osebni podatki, zlasti varovanje poklicne skrivnosti.

[15] Glej člen 9(2)(h) Splošne uredbe o varstvu podatkov.

39 Nazadnje Evropski odbor za varstvo podatkov meni, da je treba pred uvedbo takega orodja izvesti oceno učinka v zvezi z varstvom podatkov, saj se obdelava šteje za verjetno veliko tveganje (zdravstveni podatki, predvideno obsežno sprejetje, sistematično spremljanje, uporaba nove tehnološke rešitve)[16]. Evropski odbor za varstvo podatkov močno priporoča, da se ocene učinka v zvezi z varstvom podatkov objavijo.

3.2 Priporočila in funkcionalne zahteve

40 V skladu z načelom najmanjšega obsega podatkov, poleg drugih ukrepov vgrajenega in privzetega varstva podatkov[17], bi bilo treba podatke, ki se obdelujejo, zmanjšati na absolutni minimum. Aplikacija ne bi smela zbirati nepovezanih ali nepotrebnih informacij, ki lahko vključujejo osebno stanje, komunikacijske identifikatorje, sezname naprav, sporočila, dnevnike klicev, lokacijske podatke, identifikatorje naprav itd.

41 Podatki, ki jih oddaja aplikacija, morajo vključevati samo edinstvene in psevdonimne identifikatorje, ki jih aplikacija ustvari in ki so zanjo specifični. Te identifikatorje je treba redno obnavljati, in sicer tako pogosto, kot je združljivo z namenom zajezitve širjenja virusa in zadostno za omejitev tveganja identifikacije in fizičnega sledenja posameznikom.

42 Izvajanje sledenja stikom lahko sledi centraliziranemu ali decentraliziranemu pristopu[18]. Oba pristopa bi bilo treba šteti za izvedljivi možnosti, pod pogojem, da so vzpostavljeni ustrezni varnostni ukrepi, vsak pristop pa ima prednosti in slabosti. V konceptualni fazi razvoja aplikacije bi bilo zato treba vedno temeljito proučiti oba koncepta ter pri tem skrbno pretehtati njune učinke na varstvo podatkov/zasebnost in morebitne učinke na pravice posameznikov.

43 Vsak strežnik, vključen v sistem sledenja stikom, mora samo na podlagi prostovoljne privolitve uporabnika zbirati zgodovino stikov ali psevdonimne identifikatorje uporabnika, ki so mu zdravstveni organi na podlagi ustrezne ocene diagnosticirali okužbo. Druga možnost je, da mora strežnik hraniti seznam psevdonimnih identifikatorjev okuženih uporabnikov ali njihovo zgodovino stikov samo za čas, ki je potreben za obveščanje potencialno okuženih uporabnikov o njihovi izpostavljenosti, in ne sme poskušati identificirati potencialno okuženih uporabnikov.

44 Za vzpostavitev globalne metodologije za sledenje stikom, ki bo vključevala tako aplikacije kot tudi ročno sledenje, bo morda treba v nekaterih primerih obdelati dodatne informacije. V zvezi s tem bi morale te dodatne informacije ostati na terminalski napravi uporabnika in bi jih bilo treba obdelati le, če je to nujno potrebno ter s predhodno izrecno privolitvijo uporabnika.

45 Za zavarovanje podatkov, shranjenih na strežnikih in v aplikacijah, ter izmenjav med aplikacijami in oddaljenim strežnikom je treba uporabljati najsodobnejše šifrirne tehnike. Opraviti je treba tudi vzajemno avtentikacijo med aplikacijo in strežnikom.

46 Evidentiranje uporabnikov kot okuženih z virusom SARS-CoV-2 v aplikaciji mora potekati z ustreznim dovoljenjem, na primer s kodo za enkratno uporabo, ki je vezana na psevdonimno identiteto okužene osebe in povezana s postajo za testiranje ali zdravstvenim delavcem. Če potrditve ni mogoče dobiti na varen način, se ne bi smela izvesti nobena obdelava podatkov, pri kateri se predpostavlja veljavnost statusa uporabnika.

47 Upravljavec mora v sodelovanju z javnimi organi jasno in izrecno zagotoviti povezavo za prenos uradne nacionalne aplikacije za sledenje stikom, da se ublaži tveganje, da posamezniki uporabijo zunanjo aplikacijo.

---

[16] Glej Smernice Delovne skupine iz člena 29 (ki jih je sprejel Evropski odbor za varstvo podatkov) glede ocene učinka v zvezi z varstvom podatkov in opredelitve, ali je „verjetno, da bi [obdelava] povzročila veliko tveganje“, za namene Uredbe (EU) 2016/679.

[17] Glej Smernice Evropskega odbora za varstvo podatkov št. 4/2019 o členu 25 – Vgrajeno in privzeto varstvo podatkov.

[18] Na splošno je decentralizirana rešitev bolj v skladu z načelom najmanjšega obsega podatkov.

4 ZAKLJUČEK

48 Svet se spopada s hudo krizo na področju javnega zdravja, ki zahteva odločne odzive, katerih posledice se bodo čutile tudi zunaj teh izrednih razmer. Avtomatizirana obdelava podatkov in digitalne tehnologije so lahko ključni elementi v boju proti COVID-19. Potrebna pa je previdnost zaradi „zaskočnega učinka“. Zagotoviti moramo, da je vsak ukrep, ki se sprejme v teh izrednih razmerah, potreben, časovno omejen in minimalnega obsega ter podvržen rednemu in dejanskemu pregledu ter znanstveni presoji.

49 Evropski odbor za varstvo podatkov poudarja, da ne bi smelo priti do tega, da bi se bilo treba odločiti med učinkovitim odzivom na sedanjo krizo in varstvom naših temeljnih pravic; dosežemo lahko oboje, načela varstva podatkov pa lahko imajo zelo pomembno vlogo v boju proti virusu. Evropska zakonodaja o varstvu podatkov omogoča odgovorno uporabo osebnih podatkov za namene upravljanja zdravja, če je zagotovljeno, da pravice in svoboščine posameznikov v tem procesu niso ogrožene.

Za Evropski odbor za varstvo podatkov

Predsednica

(Andrea Jelinek)

PRILOGA – APLIKACIJE ZA SLEDENJE STIKOM
VODNIK ZA ANALIZO

0. Izjava o omejitvi odgovornosti

Naslednje usmeritve niso niti zavezujoče niti izčrpne. Edini namen tega vodnika je zagotoviti splošne usmeritve razvijalcem in izvajalcem aplikacij za sledenje stikom. Poleg tukaj opisanih rešitev se lahko uporabijo tudi druge rešitve, ki so zakonite, dokler so skladne z ustreznim pravnim okvirom (tj. s Splošno uredbo o varstvu podatkov in Direktivo).

Opozoriti je treba tudi, da je ta vodnik splošen. Zato se njegova priporočila in obveznosti ne smejo šteti za izčrpna. Vsako presojo je treba opraviti za vsak primer posebej, za posebne aplikacije pa bodo morda potrebni dodatni ukrepi, ki niso vključeni v ta vodnik.

1. Povzetek

V številnih državah članicah deležniki razmišljajo o uporabi aplikacij za *sledenje stikom*, ki bi prebivalcem in prebivalkam pomagale ugotoviti, ali so bili v stiku z osebo, ki je okužena z virusom SARS-CoV-2.

Pogoji, pod katerimi bi takšne aplikacije učinkovito pripomogle k obvladovanju pandemije, še niso določeni. Te pogoje bi bilo treba določiti pred uvedbo take aplikacije. Vendar je pomembno, da se razvojnim ekipam najprej zagotovijo smernice z relevantnimi informacijami, da se varstvo osebnih podatkov lahko zagotovi že v zgodnji fazi oblikovanja.

Opozoriti je treba, da je ta vodnik splošne narave. Zato se njegova priporočila in obveznosti ne smejo šteti za izčrpna. Vsako presojo je treba opraviti za vsak primer posebej, za posebne aplikacije pa bodo morda potrebni dodatni ukrepi, ki v ta vodnik niso vključeni. Namen tega vodnika je zagotoviti splošne usmeritve razvijalcem in izvajalcem aplikacij za sledenje stikom.

Nekatera merila lahko presegajo stroge zahteve, ki izhajajo iz okvira za varstvo podatkov. Njihov cilj je zagotoviti najvišjo raven preglednosti, da se spodbudi družbeno sprejemanje takih aplikacij za sledenje stikom.

Zato bi morali izdajatelji aplikacij za sledenje stikom upoštevati naslednja merila:

- Uporaba take aplikacije mora biti izključno prostovoljna. Dostop do pravic, zagotovljenih z zakonom, ne sme biti odvisen od uporabe take aplikacije. Posamezniki morajo imeti ves čas popoln nadzor nad svojimi podatki in možnost proste izbire, ali bodo tako aplikacijo uporabljali ali ne.
- Aplikacije za sledenje stikom verjetno povzročajo veliko tveganje za pravice in svoboščine posameznikov in pred njihovo uvedbo je treba izvesti oceno učinka v zvezi z varstvom podatkov.
- Informacije o medsebojni bližini uporabnikov aplikacije se lahko pridobijo brez lociranja uporabnikov. Podatki o lokaciji za tako aplikacijo niso potrebni in zato ne bi smeli biti vključeni.
- Kadar se uporabniku diagnosticira okužba z virusom SARS-CoV-2, bi bilo treba o tem obvestiti le osebe, s katerimi je bil uporabnik v tesnem stiku v epidemiološko relevantnem obdobju hrambe podatkov za sledenje stikom.

- Za delovanje take aplikacije je lahko glede na izbrano arhitekturo potrebna uporaba centraliziranega strežnika. V takem primeru ter v skladu z načeloma najmanjšega obsega podatkov in vgrajenega varstva podatkov bi morali biti podatki, ki jih obdeluje centralizirani strežnik, kar najbolj omejeni:
  - kadar se uporabniku diagnosticira okužba, se lahko informacije o njegovih predhodnih tesnih stikih ali identifikatorji, ki jih oddaja njegova aplikacija, zbirajo samo z njegovim soglasjem. Določiti je treba metodo preverjanja, s katero se lahko potrdi, da je uporabnik dejansko okužen, ne da bi prišlo do njegove identifikacije. S tehničnega vidika bi bilo to mogoče doseči tako, da se opozorilo pošlje stikom šele po posegu zdravstvenega delavca, na primer z uporabo posebne enkratne kode;
  - informacije, shranjene na centralnem strežniku, upravljavcu ne bi smele omogočati, da identificira uporabnike, ki jim je diagnosticirana okužba ali ki so bili v stiku z okuženimi uporabniki, niti ne bi smele omogočati sklepanja o vzorcih stikov, ki niso potrebni za ugotovitev relevantnih stikov.
- Za delovanje take aplikacije je potrebno oddajanje podatkov, ki jih berejo naprave drugih uporabnikov, in prejemanje tako oddanih podatkov:
  - dovolj je, da mobilna oprema uporabnikov (računalniki, tablični računalniki, povezane ročne ure itd.) izmenjuje psevdonimne identifikatorje, na primer z oddajanjem (npr. prek tehnologije nizkoenergijskega Bluetootha);
  - identifikatorji morajo biti generirani z uporabo najsodobnejših šifrirnih postopkov;
  - identifikatorje je treba redno obnavljati, da se zmanjša tveganje fizičnega sledenja in napadov s ciljem vnovične identifikacije.
- Taka aplikacija mora biti zavarovana, da se zagotovi varnost tehničnih postopkov. Zlasti velja naslednje:
  - aplikacija uporabnikom ne bi smela posredovati informacij, ki bi jim omogočale sklepanje o identiteti ali diagnozi drugih uporabnikov. Centralni strežnik ne sme niti identificirati uporabnikov niti izpeljevati zaključkov iz informacij o njih.

Izjava o omejitvi odgovornosti: zgoraj navedena načela se nanašajo izključno na navedeni namen aplikacij za *sledenje stikom*, ki so namenjene samo samodejnemu obveščanju oseb, potencialno izpostavljenih virusu (ne da bi bilo treba te osebe identificirati). Operaterje aplikacije in njeno infrastrukturo lahko nadzira pristojni nadzorni organ. Upoštevanje vseh smernic ali njihovega dela ne zadostuje nujno za zagotovitev popolne skladnosti z okvirom varstva podatkov.

2. Opredelitev pojmov

Stik	Za namene aplikacije za sledenje stikom pomeni stik uporabnika, ki je bil v interakciji z uporabnikom, za katerega je potrjeno, da je nosilec virusa, in pri katerem zaradi trajanja interakcije in razdalje obstaja tveganje znatne izpostavljenosti okužbi z virusom. Parametre trajanja izpostavljenosti in razdalje med osebami morajo oceniti zdravstveni organi in ti parametri se lahko namestijo v aplikaciji.

Lokacijski podatki	Lokacijski podatki pomenijo vse podatke, obdelane v elektronskem komunikacijskem omrežju ali v okviru elektronske komunikacijske storitve, ki razkrivajo zemljepisni položaj terminalske opreme uporabnika javno razpoložljive elektronske komunikacijske storitve (kot so opredeljeni v Direktivi), in podatke iz morebitnih drugih virov, ki se nanašajo na: - zemljepisno širino, dolžino ali višino terminalske opreme; - smer potovanja uporabnika ali - čas beleženja informacij o lokaciji.
Interakcija	V okviru aplikacije za sledenje stikom je interakcija opredeljena kot izmenjava informacij med dvema napravama, ki sta v neposredni bližini (prostorsko in časovno), znotraj dosega uporabljene komunikacijske tehnologije (npr. Bluetooth). Ta opredelitev ne vključuje lokacije obeh uporabnikov v interakciji.
Nosilec virusa	V tem dokumentu je nosilec virusa uporabnik, pri katerem je bil rezultat testiranja na virus pozitiven in ki je od zdravnika ali zdravstvenega centra prejel uradno diagnozo.
Sledenje stikom	Pri osebah, ki so bile v tesnem stiku (v skladu z merili, ki jih opredelijo epidemiologi) s posameznikom, ki je okužen z virusom, obstaja znatno tveganje, da so prav tako okužene in da lahko okužijo druge. Sledenje stikom je metodologija za obvladovanje bolezni, pri kateri se ustvari seznam vseh oseb, ki so bile v neposredni bližini nosilca virusa, da se preveri, ali pri njih obstaja tveganje okužbe, in da se v zvezi z njimi sprejmejo ustrezni sanitarni ukrepi.

3. Splošno

GEN-1	Aplikacija mora dopolnjevati tradicionalne tehnike sledenja stikom (kot so zlasti pogovori z okuženimi osebami), tj. mora biti del širšega programa javnega zdravja. Uporabljati se sme samo do takrat, ko lahko tehnike ročnega sledenja stikom same obvladujejo število novih okužb.
GEN-2	Najpozneje takrat, ko pristojni javni organi sprejmejo odločitev o „vrnitvi v normalno stanje“, je treba vzpostaviti postopek, da se konča zbiranje identifikatorjev (globalna deaktivacija aplikacije, navodila za odstranitev aplikacije, samodejna odstranitev itd.) in aktivira izbris vseh zbranih podatkov iz vseh podatkovnih zbirk (mobilnih aplikacij in strežnikov).
GEN-3	Izvorna koda aplikacije in njenega zaledja mora biti odprta, tehnične specifikacije pa morajo biti objavljene, da lahko vsaka zadevna stran kodo preveri in po potrebi prispeva k izboljšanju kode, odpravi morebitnih napak ter zagotovitvi preglednosti obdelave osebnih podatkov.

GEN-4	Faze uvajanja aplikacije morajo omogočiti postopno potrditev njene učinkovitosti z vidika javnega zdravja. V ta namen je treba najprej določiti evalvacijski protokol s kazalniki, ki omogočajo merjenje učinkovitosti aplikacije.

4. Nameni

PUR-1	Aplikacija mora biti namenjena izključno sledenju stikom, da je mogoče opozoriti osebe, ki so potencialno izpostavljene virusu SARS-CoV-2, in poskrbeti zanje. Ne sme se uporabljati za noben drug namen.
PUR-2	Aplikacija se ne sme od primarnega namena uporabe preusmeriti v namene spremljanja spoštovanja ukrepov karantene ali osamitve in/ali omejevanja socialnih stikov.
PUR-3	Aplikacija se ne sme uporabljati za oblikovanje zaključkov o lokaciji uporabnikov na podlagi njihove interakcije in/ali drugih sredstev.

5. Funkcionalni vidiki

FUNC-1	Aplikacija mora imeti funkcijo, ki uporabnikom omogoča, da so obveščeni o tem, da so bili potencialno izpostavljeni virusu, pri čemer ta informacija temelji na tem, da so bili v bližini okuženega uporabnika v obdobju X dni pred pozitivnim presejalnim testom (vrednost X opredelijo zdravstveni organi).
FUNC-2	Aplikacija bi morala dati priporočila uporabnikom, za katere je ugotovljeno, da so bili potencialno izpostavljeni virusu. Uporabnikom bi morala dati navodila v zvezi z ukrepi, ki bi jih morali upoštevati, navodila pa bi morala uporabnikom omogočiti, da zaprosijo za nasvet. V takih primerih bi bilo obvezno človekovo posredovanje.
FUNC-3	Algoritem, ki meri tveganje okužbe, pri čemer upošteva dejavnika razdalje in časa, ter tako določi, kdaj mora biti stik zabeležen v seznamu za sledenje stikom, mora biti varno nastavljiv, da se upošteva najnovejše znanje o širjenju virusa.
FUNC-4	**Uporabniki morajo biti** v inkubacijski dobi virusa **obveščeni, če so bili izpostavljeni virusu**, ali pa morajo redno prejemati informacije o tem, ali so bili izpostavljeni virusu ali ne.
FUNC-5	Aplikacija bi morala biti interoperabilna z drugimi aplikacijami, razvitimi v državah članicah, da bodo lahko uporabniki, ki potujejo po različnih državah članicah, učinkovito obveščeni.

6. Podatki

DATA-1	Da se lahko izvaja sledenje stikom, mora biti aplikacija zmožna oddajati in prejemati podatke prek komunikacijskih tehnologij, ki temeljijo na bližini, kot je nizkoenergijski Bluetooth (*Bluetooth Low Energy*).
DATA-2	Ti podatki, ki jih oddaja aplikacija, morajo vključevati šifrirno močne psevdonaključne identifikatorje, ki jih generira aplikacija in so zanjo specifični.
DATA-3	Tveganje kolizije med psevdonaključnimi identifikatorji bi moralo biti dovolj nizko.
DATA-4	Psevdonaključne identifikatorje je treba redno obnavljati, in sicer tako pogosto, da se omeji tveganje, da kdor koli, vključno z operaterji centralnega strežnika, drugimi uporabniki aplikacije ali zlonamernimi tretjimi osebami, izvede vnovično identifikacijo, fizično sledenje ali povezovanje posameznikov. Te identifikatorje mora generirati aplikacija uporabnika, po možnosti na podlagi serije (*seed*), ki jo zagotovi centralni strežnik.
DATA-5	V skladu z načelom najmanjšega obsega podatkov aplikacija ne sme zbirati podatkov, ki niso nujno potrebni za namen sledenja stikom.
DATA-6	Aplikacija ne sme zbirati lokacijskih podatkov za namen sledenja stikom. Lokacijski podatki se lahko obdelajo samo zato, da bi se aplikaciji omogočila interakcija s podobnimi aplikacijami v drugih državah, in ta obdelava bi morala biti natančno omejena na to, kar je nujno za ta izključni namen.
DATA-7	Aplikacija ne bi smela zbirati zdravstvenih podatkov poleg tistih, ki so nujno potrebni za njene namene, razen na prostovoljni podlagi in z izključnim namenom pomoči v postopku odločanja o obveščanju uporabnika.
DATA-8	Uporabnike je treba obvestiti o vseh osebnih podatkih, ki se bodo zbirali. Te podatke bi bilo treba zbirati le z dovoljenjem uporabnika.

7. Tehnične lastnosti

TECH-1	Aplikacija bi morala uporabljati razpoložljive tehnologije, kot je komunikacijska tehnologija, ki temelji na bližini (npr. nizkoenergijski Bluetooth), da se odkrijejo uporabniki v bližini naprave, na kateri je aplikacija.
TECH-2	Aplikacija bi morala v opremi hraniti zgodovino stikov uporabnika, in sicer za vnaprej določeno omejeno obdobje.
TECH-3	Aplikacija se za izvedbo nekaterih svojih funkcij lahko opira na centralni strežnik.
TECH-4	Aplikacija mora temeljiti na arhitekturi, ki se čim bolj opira na naprave uporabnikov.
TECH-5	Na zahtevo uporabnikov, ki so evidentirani kot okuženi z virusom, in po tem, ko njihov status potrdi ustrezno certificirani zdravstveni delavec, bi bilo treba njihovo zgodovino stikov ali njihove lastne identifikatorje prenesti na centralni strežnik.

8. Varnost

SEC-1	Obstajati mora mehanizem za preverjanje statusa uporabnikov, ki so v aplikaciji evidentirani kot pozitivni na SARS-CoV-2, na primer s pošiljanjem kode za enkratno uporabo, povezane s postajo za testiranje ali zdravstvenim delavcem. Če potrditve ni mogoče dobiti varno, se podatki ne smejo obdelati.
SEC-2	Podatki, poslani na centralni strežnik, se morajo prenesti prek varnega kanala. Uporabo storitev obveščanja, ki jih zagotavljajo ponudniki odprtokodne platforme, bi bilo treba skrbno oceniti in ta uporaba ne bi smela povzročiti razkritja kakršnih koli podatkov tretjim osebam.
SEC-3	Zahteve ne smejo biti dovzetne za nedovoljene posege zlonamernega uporabnika.
SEC-4	Za zavarovanje izmenjav med aplikacijo in strežnikom ter med aplikacijami in za splošno zaščito informacij, shranjenih v aplikacijah in na strežniku, je treba uporabljati najsodobnejše šifrirne tehnike. Primeri tehnik, ki se lahko uporabijo, so: simetrično in asimetrično šifriranje, zgoščevalne funkcije (*hash functions*), šifrirni protokoli PMT (*private membership test*), PSI (*private set intersection*) in PIR (*private information retrieval*), Bloomovi filtri, homomorfno šifriranje itd.
SEC-5	Centralni strežnik ne sme hraniti identifikatorjev omrežnih povezav (npr. naslovov IP) nobenega uporabnika, vključno z uporabniki s pozitivno diagnozo in tistimi, ki so na strežnik prenesli svojo zgodovino stikov ali svoje lastne identifikatorje.
SEC-6	Da bi se izognili izdajanju za drugo osebo ali ustvarjanju lažnih uporabnikov, mora strežnik aplikacijo avtenticirati.
SEC-7	Aplikacija mora avtenticirati centralni strežnik.
SEC-8	Funkcije strežnika bi bilo treba zaščititi pred napadi s ponavljanjem.
SEC-9	Informacije, ki jih prenaša centralni strežnik, morajo biti podpisane, da se avtenticira njihov izvor in celovitost.
SEC-10	Dostop do vseh podatkov, ki so shranjeni na centralnem strežniku in niso javno dostopni, mora biti omejen samo na pooblaščene osebe.
SEC-11	Upravljavec dovoljenj naprave na ravni operacijskega sistema sme zahtevati le dovoljenja za dostop do komunikacijskih modulov in njihovo uporabo, kadar je to potrebno, za shranjevanje podatkov na terminalski napravi ter za izmenjavo informacij s centralnim strežnikom.

9. Varstvo osebnih podatkov in zasebnosti posameznikov

Opomnik: naslednje smernice se nanašajo na aplikacijo, katere edini namen je sledenje stikom.

PRIV-1	Pri izmenjavah podatkov je treba spoštovati zasebnost uporabnikov (in zlasti načelo najmanjšega obsega podatkov).
PRIV-2	Aplikacija ne sme omogočati neposredne identifikacije uporabnikov, ko uporabljajo aplikacijo.
PRIV-3	Aplikacija ne sme omogočati sledenja gibanju uporabnikov.
PRIV-4	Uporaba aplikacije uporabnikom ne bi smela omogočati, da izvejo kar koli o drugih uporabnikih (zlasti to, ali so nosilci virusa ali ne).
PRIV-5	Zaupanje v centralni strežnik mora biti omejeno. Upravljanje centralnega strežnika mora potekati v skladu z jasno opredeljenimi pravili upravljanja in vključevati vse potrebne ukrepe za zagotovitev njegove varnosti. Lokalizacija centralnega strežnika bi morala omogočiti učinkovit nadzor s strani pristojnega nadzornega organa.
PRIV-6	Izvesti je treba oceno učinka v zvezi z varstvom podatkov in jo objaviti.
PRIV-7	Aplikacija bi morala uporabniku razkriti samo, ali je bil izpostavljen virusu ter, po možnosti brez razkrivanja informacij o drugih uporabnikih, število in datume izpostavljenosti.
PRIV-8	Informacije, ki jih prenaša aplikacija, uporabnikom ne smejo omogočati identifikacije uporabnikov, ki so nosilci virusa, niti sledenja njihovemu gibanju.
PRIV-9	Informacije, ki jih prenaša aplikacija, zdravstvenim organom ne smejo omogočati identifikacije potencialno izpostavljenih uporabnikov brez njihovega soglasja.
PRIV-10	Zahteve iz aplikacije, naslovljene na centralni strežnik, ne smejo razkriti ničesar o nosilcu virusa.
PRIV-11	Zahteve iz aplikacije, naslovljene na centralni strežnik, ne smejo razkriti nobenih nepotrebnih informacij o uporabniku, razen in samo, kadar je to potrebno, njegovih psevdonimnih identifikatorjev in njegovega seznama stikov.
PRIV-12	Napadi s ciljem ponovne identifikacije ne smejo biti mogoči.
PRIV-13	Uporabniki morajo imeti možnost, da prek aplikacije uveljavljajo svoje pravice.
PRIV-14	Posledica izbrisa aplikacije mora biti izbris vseh lokalno zbranih podatkov.
PRIV-15	Aplikacija bi morala zbirati samo podatke, ki jih prenaša ista aplikacija z druge naprave ali interoperabilna enakovredna aplikacija. Zbirati se ne smejo nobeni podatki, ki so povezani z drugimi aplikacijami in/ali napravami za komunikacijo na podlagi bližine.
PRIV-16	Da bi se izognili ponovni identifikaciji s strani centralnega strežnika, bi bilo treba uporabljati posredniške strežnike. Namen teh *verodostojnih strežnikov* je pomešati identifikatorje več uporabnikov (tako nosilcev virusa kot tudi vložnikov zahtev) pred njihovim prenosom na centralni strežnik, da se prepreči, da centralni strežnik pozna identifikatorje (kot so naslovi IP) uporabnikov.

PRIV-17	Aplikacijo in strežnik je treba skrbno razviti in nastaviti, da se ne bi zbirali nepotrebni podatki (npr. v strežniške dnevnike ne bi smeli biti vključeni identifikatorji itd.) in da bi se preprečila uporaba paketa za razvoj programske opreme (SDK) tretje osebe, ki zbira podatke za druge namene.

Večina aplikacij za sledenje stikom, o katerih se trenutno razpravlja, pravzaprav sledi dvema pristopoma, ko se potrdi, da je uporabnik okužen: na strežnik pošljejo bodisi zgodovino stikov tega uporabnika, ki so jo pridobile s skeniranjem, bodisi seznam lastnih identifikatorjev, ki jih je aplikacija oddajala. Naslednja načela so predstavljena v skladu s tema dvema pristopoma. Dejstvo, da sta tukaj obravnavana ta pristopa, ne pomeni, da drugi pristopi niso mogoči ali celo ustreznejši, na primer pristopi, ki uporabljajo neko obliko šifriranja E2E ali druge tehnologije za povečevanje varnosti ali boljše varovanje zasebnosti.

9.1. **Načela, ki se uporabljajo** samo, **kadar aplikacija pošlje na strežnik seznam stikov:**

CON-1	Centralni strežnik mora zbirati zgodovino stikov uporabnikov, ki so evidentirani kot pozitivni na SARS-CoV-2, samo če so uporabniki v to prostovoljno privolili.
CON-2	Centralni strežnik ne sme niti hraniti niti širiti seznama psevdonimnih identifikatorjev uporabnikov, ki so nosilci virusa.
CON-3	Zgodovino stikov, ki je shranjena na centralnem strežniku, je treba izbrisati, ko so uporabniki obveščeni o tem, da so bili v bližini osebe s pozitivno diagnozo.
CON-4	Razen če uporabnik, ki je potrjen kot pozitiven, deli svojo zgodovino stikov s centralnim strežnikom ali če neki uporabnik strežniku pošlje zahtevo, da bi ugotovil svojo potencialno izpostavljenost virusu, se z opreme uporabnika ne smejo pridobiti nobeni podatki.
CON-5	Vsak identifikator, vključen v lokalno zgodovino, je treba izbrisati po X dneh od njegovega zbiranja (vrednost X določijo zdravstveni organi).
CON-6	Zgodovine stikov, ki jih predložijo različni uporabniki, se ne smejo nadalje obdelovati, na primer z navzkrižno korelacijo, da bi se izdelali globalni zemljevidi bližine.
CON-7	Podatki v strežniških dnevnikih morajo biti čim manjšega obsega in izpolnjevati zahteve glede varstva podatkov.

9.2. Načela, ki se uporabljajo samo, kadar aplikacija pošlje na strežnik seznam lastnih identifikatorjev:

ID-1	Centralni strežnik mora zbirati identifikatorje, ki jih oddaja aplikacija, uporabnikov, ki so evidentirani kot pozitivni na SARS-CoV-2, samo če so uporabniki v to prostovoljno privolili.
ID-2	Centralni strežnik ne sme hraniti niti širiti zgodovine stikov uporabnikov, ki so nosilci virusa.
ID-3	Identifikatorje, ki so shranjeni na centralnem strežniku, je treba izbrisati, ko se prenesejo drugim aplikacijam.

ID-4	Razen če uporabnik, ki je potrjen kot pozitiven, deli svoje identifikatorje s centralnim strežnikom ali če neki uporabnik strežniku pošlje zahtevo, da bi ugotovil svojo potencialno izpostavljenost virusu, se z opreme uporabnika ne smejo pridobiti nobeni podatki.
ID-5	Podatki v strežniških dnevnikih morajo biti čim manjšega obsega in izpolnjevati zahteve glede varstva podatkov.